UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA

PAUL KRAMER, on behalf of himself and all others similarly situated, Plaintiff v. APRIA HEALTHCARE, LLC, Defendant	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Paul Kramer ("Kramer"), by and through his attorneys of record, upon personal knowledge as to his own acts and experiences, and upon information and belief as to all other matters, brings this class action complaint against defendant Apria Healthcare, LLC ("Apria" or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant Apria for its failure to properly secure and safeguard Plaintiff's and Class Members' protected medical and health information stored within Defendant's information network and servers, including, without limitation,

protected health information" or "PHI",1 and "personally identifiable information" or "PII",2 as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Apria provides home healthcare equipment, including equipment and supplies for the treatment of sleep apnea, wound care, diabetes, and pharmacy services. Apria provides services and supplies to approximately two million consumers throughout the United States. Apria is headquartered in Indianapolis, Indiana and operates out of approximately 275 locations in the United States.[3] In the course of providing these services Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and PHI to facilitate the healthcare-related services Plaintiff and Class Members requested or received. Defendant knew, at all times material, that it was collecting and storing, and responsible for the security of sensitive data, including Plaintiff's and Class Members' highly confidential PII and PHI.

3. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and more than 1.8 million other similarly situated persons by virtue of two massive and preventable cyberattacks that began no later than April 5, 2019, continuing until May 7, 2019, and then occurred again between August 27, 2021, to October 10, 2021, by which

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] www.apria.com (last visited June 12, 2023).

cybercriminals infiltrated Apria's computer system on which the Private Information that Defendant was entrusted with and responsible for, was stored (the "Data Breach"). Plaintiff further seeks to hold Defendant responsible for not ensuring that the PII and PHI was maintained in a manner consistent with industry standards, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), and other relevant standards.

4. Defendant knew or should have known of the cyber-attack by no later than September 1, 2021. Nonetheless, Defendant waited until June 2023, approximately one year and nine months, to inform victims of the Data Breach. Indeed, Plaintiff and Class Members did not begin to receive notification letters from Defendant informing them of the Data Breach (the "Notice"), until commencing on or about June 6, 2023, and at various times thereafter.

5. HIPAA establishes obligations for the protection of individuals' medical records and other personal health information. HIPAA, in general, applies to healthcare providers, health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets requirements for Defendant's maintenance of Plaintiff's and Class Members' PII and PHI. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of patient health information and sets limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization. HIPAA also gives a series of rights to patients over their PII and PHI, including rights to examine and obtain copies of their health records, and to request corrections thereto.

6. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

7. By obtaining, collecting, storing, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

These duties arise from HIPAA and other state and federal statutes and regulations, as well as common law principles. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining PHI and imposes a duty on Defendant to maintain the confidentiality of such information. Defendant is charged, *inter alia*, with legal violations predicated upon the duties set forth in HIPAA that underpin those violations and that were not honored, or were otherwise breached by Apria.

8. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiff and Class Members were compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future – and are entitled to damages. In addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Paul Kramer

9. Plaintiff Kramer is, and at all relevant times was, a resident of Lake Forest, California. While insured through his former employer, Plaintiff Kramer received services and supplies from Apria for several years, including, *inter alia*, supplies for a nebulizer and a continuous positive airway pressure ("CPAP") machine. Plaintiff Kramer has not received services or supplies from Apria since at least 2020. Plaintiff Kramer received a Notice of Data Breach, dated June 6, 2023, stating that his "date of birth, device descriptions, patient account number, patient address, patient dates of service, patient email address, patient name, and patient phone

numbers" may have been exposed in the Data Breach. A copy of the Notice of Data Breach received by Plaintiff Kramer is attached hereto as Exhibit A.

Defendant Apria Healthcare, LLC

10. Defendant Apria provides home healthcare equipment, including equipment and supplies for the treatment of sleep apnea, wound care, diabetes, and pharmacy services. Apria provides services and supplies to approximately two million consumers throughout the United States. Apria is headquartered at 7353 Company Drive, Indianapolis, Indiana and operates out of approximately 275 locations in the United States.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, the nationwide and California classes include recipients of Defendant's Notice of Data Breach, which, upon information and belief, include non-Indiana citizens. Since Defendant is an Indiana-based entity headquartered in Indianapolis, there is minimal diversity between at least one member of the Plaintiff's nationwide class and Defendant.

12. This Court also has subject matter jurisdiction over this case pursuant to 28. U.S.C. § 1331 because several of the claims for relief herein are dependent or predicted upon violating duties imposed upon Apria by federal law and regulation, including HIPAA, as more fully alleged below.

13. This Court has general personal jurisdiction over Defendant because Defendant operates its principal place of business in Indianapolis, Indiana. Additionally, this Court also has specific personal jurisdiction over Defendant because it has minimum contacts with Indiana, as it is located and conducts substantial business in or from Indiana.

14. This Court has supplemental jurisdiction over any claims not arising, in whole or in part, from violation of federal law.

15. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial part of its business within this District.

FACTUAL BACKGROUND

The Data Breach

16. On or about June 6, 2023, Defendant sent Plaintiff and other victims of the Data Breach a Notice of Data Breach ("Notice Letter"), informing them that:

> We are writing to tell you about a data breach that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.[4]

17. The Notice Letter acknowledges that Defendant learned of the Data Breach on September 1, 2021, stating that:

> On September 1, 2021, Apria Healthcare LLC ("Apria") received a notification regarding access to select Apria systems by an unauthorized third party. Apria took immediate action to mitigate the incident, including working with the Federal Bureau of Investigation (FBI) and hiring a reputable forensic investigation team to investigate and securely resolve the incident. An unauthorized third party accessed systems which contained personal information from April 5, 2019 to May 7, 2019 and from August 27,2021 to October 10, 2021.[5]

18. Despite learning of the Data Breach no later than September 2021, Defendant did not begin to inform impacted individuals after the Data Breach's occurrence, and the remedial measures undertaken to ensure such a breach does not occur again, until on or around June 6, 2023. To date, Defendant has failed to disclose the root cause of the Data Breach, the vulnerabilities exploited, why it took approximately two years and five months after the initial data breach for

[4] Exhibit A hereto.

[5] *Id.*

Apria to learn of the data breach, and why it took more than eighteen months from learning of the Data Breach to inform Class Members, each of whom has a vested interest in ensuring that their Private Information remains protected.

19. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

20. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, ultimately causing the exposure of Private Information.

21. Upon information and belief, Defendant continues to maintain Plaintiff's PHI and PII, as well as that of all other Class Members.

Apria's Business and Obligation to Preserve and Protect Confidentiality and Privacy

22. Apria provides medical supplies and services to consumers suffering from long term illnesses such as diabetes, sleep apnea, and COPD. It also provides services and equipment for wound care and enteral nutrition, such as feeding tubes and formulas. Apria is headquartered at 7353 Company Drive, Indianapolis, Indiana and operates out of approximately 275 locations in the United States.

23. Plaintiff and Class Members are current or former clients of Defendant who obtained service(s) and/or supplies through Defendant.

24. As a consequence of securing or receiving services from Defendant, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including their names, dates of birth, health information, social security numbers, financial information, insurance information, and other sensitive information.

25. Defendant's Notice of Privacy Practices acknowledges that:

> When we use or disclose your PHI, we are required to abide by the terms of this Notice (or other notice in effect at the time of the use or disclosure). This Notice

> applies to all the information about you that we obtain that relates to your past, present, or future physical or mental health or condition, the provision of healthcare products and services to you or payment for such services. [6]

26. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. The information collected by Defendant included the Private Information of Plaintiff and Class Members.

27. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII/PHI.

28. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. And to that end, Defendant also has a legal duty created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. In addition, obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

[6] https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf, last visited June 12, 2023.

30. Plaintiff is informed and believes and thereupon alleges that in order to obtain services from Defendant, Plaintiff and Class Members were required to provide sensitive personal and private healthcare information, including the Private Information compromised in the Data Breach.

31. By obtaining, collecting, using, Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. Given the highly sensitive nature of the PII and PHI it possessed and the sensitivity of the medical and health services it provides, Apria had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII and PHI.

33. As a condition to obtain medical services from Defendant, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendant.

34. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its medical services.

35. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

36. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

37. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

38. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

39. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiff's and Class Members' Private Information via the Data Breach was not permitted per Defendant's own Privacy Policy.

40. Additionally, Defendant is duty bound to adhere to its Notice of Privacy Practices relating to the Confidentiality of PHI. This policy clearly states that Apria is . . . required by law to maintain the privacy of your protected health information ('PHI')[.]" [7]

41. Even though Apria recognized that confidential and Private Information had been assessed and infiltrated on or around September 1, 2023, it was not until on or about June 6, 2023, and at various times thereafter, months later, that Defendant began sending affected parties Notice Letters.

42. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

44. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of approximately 1.8 million individuals.

[7] https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf (last visited June 12, 2023).

45. Because of Defendant's negligence and misconduct in failing to keep their information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by Unauthorized individuals who can now access the PHI and PII of Plaintiff and Class Members and use it as they please.

46. Plaintiff and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

47. The PII and PHI of consumers, such as Plaintiff and Class Members, is valuable and has been commoditized in recent years.

48. Defendant was also aware of the significant repercussions that would result from its failure to do protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security were breached. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

49. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

50. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

51. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such

sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

52. Plaintiff and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

53. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

54. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

55. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class Members' Private Information, Plaintiff and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Apria Was Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

56. As a condition of its relationships with its customers, Plaintiff and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII and PHI and financial information. Defendant, in turn, collected, stored, and maintained that information and assured consumers that it was acting to protect that PHI and PII pursuant to HIPAA and to prevent its disclosure.

57. Plaintiff and Class Members were required to provide their PII and PHI and financial information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

58. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and financial information. Plaintiff and Class Members relied on Defendant to keep their PII and PHI and financial information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

59. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

60. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII and PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity in the healthcare space, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

61. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. In 2021, a record 715 healthcare data breaches reported, an increase of approximately 100% since 2017.[8]

62. This trend continued in 2022, with 707 healthcare breaches reported, still near record highs.[9] Additionally, according to the HIPAA Journal, the five largest healthcare data breaches reported in 2022 impacted the healthcare records of approximately 13.3 million people.[10]

[8] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed June 12, 2023).

[9] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed June 12, 2023).

[10] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed June 12, 2023).

Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[11] Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[12]

63. In the context of data breaches, healthcare is "by far the most affected industry sector."[13] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[14]

64. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[15]

65. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained and collected by a healthcare entity were accessed and/or acquired by a cybercriminal.

---

[11] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed June 12, 2023).

[12] *Id*. (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[13] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed June 12, 2023).

[14] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed June 12, 2023).

[15] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed June 12, 2023).

66. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place and assure the security of the data collected by it and entrusted to it by Plaintiff and Class Members.

67. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII and PHI from being compromised.

Defendant's Conduct Violates Federal Law, Including the Rules and Regulations of HIPAA and HITECH

68. Defendant has a statutory duty under HIPAA and other federal or state statutes to safeguard Plaintiff's and Class Members' data.

69. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data under the implied condition that Defendant and its participating entities would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

70. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

71. Defendant is a covered entity pursuant to HIPAA. See 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

72. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[16] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

73. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

74. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

75. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

76. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

77. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

78. HIPAA's Security Rule requires Defendant to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[16] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by its workforce.

79. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

80. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

81. Plaintiff's and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

82. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

83. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

84. Plaintiff's and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

85. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

86. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

87. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

88. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

89. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

90. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

91. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

92. This Data Breach is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."

See 45 C.F.R. 164.40.

93. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

94. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII and PHI.

95. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy

rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

k. Retaining information past a recognized purpose and not deleting it.

96. Upon information and belief, prior to the Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiff and Class Members.

97. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

98. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

99. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII and PHI of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiff's and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

100. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and PHI and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems,

networks, and protocols adequately protected the PII and PHI and financial information of Plaintiff and Class Members.

101. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

102. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and PHI and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

103. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

104. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

105. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

106. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

107. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff's and Class Members' as a result of the Data Breach.

Defendant Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

108. Apria is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

109. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

110. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[18]

111. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

112. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

113. Apria failed to properly implement basic data security practices. ILS's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

114. Apria was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of its business model of collecting Private Information and

[17] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 23, 2023).

[18] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 12, 2023).

storing such information. Apria was also aware of the significant repercussions that would result from its failure to do so.

Value of the Relevant Sensitive Information

115. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

116. The high value of PII and PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[21]

[19] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 12, 2023).

[20] Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 12, 2023).

[21] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 12, 2023).

117. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[22] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[23] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[24]

118. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

119. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

120. Identity thieves can use PII and PHI and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's

[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed June 12, 2023).

[23] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed June 12, 2023).

[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches (last accessed June 12, 2023).

name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

121. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII and PHI are long lasting and severe. Once PII and PHI and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII and PHI of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

122. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

123. The harm to Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which

[25] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed June 12, 2023).

is more than identity thefts involving banking and finance, the government and the military, or education.[26]

124. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[27]

125. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

126. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[29]

127. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

---

[26] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed June 12, 2023).

[27] *Id.*

[28] See Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed June 12, 2023).

[29] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breachwhat-to-know-about-them-and-what-to-do-after-one/ (last accessed June 12, 2023).

[30] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

security solutions."[31] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[32]

128. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[33]

129. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards and concomitant duties mandated and required by HIPAA regulations.

Defendant's Delayed Response to the Breach

130. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers, Dates of birth, and other critical PHI and/or PII.

[31] *Id*. at 17.

[32] *Id*. at 28.

[33] *Id.*

131. Despite this understanding, Defendant did not begin informing affected individuals, including Plaintiff and Class Members, about the Data Breach until June 6, 2023. The Notice Letter provided only scant details of the Data Breach and Defendant's recommended next steps.

132. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[34]

133. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[35] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[36] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

134. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

---

[34] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimumwage/2020/home.htm#:~:text=In%202020%2C%207 3.3%20million%20workers,wage%20of%2 0%247.25%20per%20hour (last visited March 23, 2023); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/charts/employment-situation/employment-and-average-hourly-earnings-byindustry-bubble.htm (last visited March 23, 2023) (finding that on average, private-sector workers make $1,312.80 per 40-hour work week.).

[35] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-jameswallman.html (last visited June 12, 2023).

[36] *Id.*

I. CLASS ALLEGATIONS

135. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class, defined as

> All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Apria Data Breach.

136. In addition, Plaintiff Kramer asserts three statutory claims, as more fully alleged hereinafter, on behalf of a California Class, defined as follows:

> All residents of the state of California whose PII or PHI was accessed or otherwise compromised as a result of the Apria Data Breach.

Members of the Nationwide Class and the California Class are referred to herein collectively as "Class Members" or "Class."

137. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

138. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

139. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but Apria provides services to approximately two million consumers at approximately 275 locations throughout the United States.[37] Apria has acknowledged that the number of individuals affected by the Data Breach was over 1.8 million persons, indicating that there are more than 1.8 million members of the Class, making joinder of each individual impracticable.[38] Ultimately, members of the Class will be readily identified through Defendant's records.

---

[37] https://www.apria.com last visited June 12, 2023.

[38] https://apps.web.maine.gov/online/aeviewer/ME/40/bf218a4e-1ffd-4f14-a74d-3d34aec8d6c7.shtml last visited June 12, 2023.

140. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated HIPAA, federal, state and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or FTC law or regulations, imposing duties upon Apria, applicable to Plaintiff and Class Members;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Apria Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendant entered into contracts with Plaintiff and the Class Members that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of their contracts with Plaintiff and each of the Class Members;

j) Whether Defendant should retain the money paid by Plaintiff and each of the Class Members to protect their PII and PHI;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

141. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

142. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

143. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Apria still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PHI and PII collected, stored, and maintained by Defendant.

144. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

145. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On Behalf of Plaintiff, the Nationwide Class, and California Class)

146. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

147. Plaintiff and Class Members were required to submit PII and PHI to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

148. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

149. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose PII and PHI had been entrusted to Defendant.

150. Defendant breached its duty to Plaintiff and Class Members by failing to secure their PII and PHI from unauthorized disclosure to third parties.

151. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII and PHI.

152. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII and PHI of Plaintiff and the Class Members.

153. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

154. Because of Defendant's wrongful and negligent breach of its duty to Plaintiff and the Class Members, they have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

155. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of such duties would cause Plaintiff and Class

Members to experience the foreseeable harms associated with the unauthorized exposure of their PII and PHI.

156. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff, the Nationwide Class, and California Class)

157. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

158. Defendant is a covered entity pursuant to HIPAA, *see* 45 C.F.R. § 160.102, and pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

159. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

160. As persons who shared their "protected health information" with Defendant, Plaintiff and Class Members are in the class of persons for whose protection HIPAA was enacted to protect.

161. Defendant breached its duty to Plaintiff and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI from unauthorized access.

162. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

163. Defendant's wrongful and negligent breach of its duty was the proximate cause of the injury to Plaintiff and Class Members, and the injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that

duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII and PHI.

164. Because of Defendant's wrongful and negligent breach of its duty to Plaintiff and the Class Members, they have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

165. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

166. In the alternative, and as a further basis for this claim, as alleged in Count VI below, Defendant's conduct violated the California Confidentiality of Medical Information Act, and Defendant's violation of the statute constitutes negligence *per se*.

COUNT III
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff, the Nationwide Class, and California Class)

167. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

168. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendant, as alleged above.

169. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take

reasonable measures to protect Plaintiff's PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

170. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who sought medical services from Apria and, in doing so, entrusted Defendant, pursuant to its requirements and Privacy Notice, with their PII and PHI.

171. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII and PHI.

172. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

173. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

174. Accordingly, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff, the Nationwide Class, and the California Class)

175. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

176. Defendant accepted the special confidence placed in its by Plaintiff and Class Members. There was an understanding between the parties that the healthcare service provider Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their PII and PHI.

177. Defendant became the guardian of Plaintiff's and Class Members' PII and PHI and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' PII and PHI.

178. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of Defendant's medical relationship with its patients, in particular, to keep secure the PII and PHI of those patients.

179. Defendant breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect their PII and PHI; (b) by failing to notify Plaintiff and the Class Members of the unauthorized disclosure of the PII and PHI; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII and PHI.

180. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII and PHI; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiff's and Class Members' PII and PHI.

181. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, and the California Class)

182. Plaintiff, on behalf of himself and the Class, re-alleges and incorporates the above allegations by reference.

183. Defendant collected and maintained responsibility for the Private Information of Plaintiff and the Class, including, *inter alia*, name, date of birth, address, Medicare identification number, health care subscriber identification number, and other PII in connection with the provision of services to Plaintiff and the Class.

184. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not

take unjustified risks when storing the PII.

185. Plaintiff and the Class would not have entrusted their PHI and PII to Defendant had they known that Defendant would fail to adequately safeguard their PHI and PII.

186. At the time when Plaintiff and Class members entrusted Defendant with their PHI and PII, Defendant published the HIPAA Rights Notice, agreeing to protect and keep private financial information of Plaintiff and the Class.

187. Implicit in the agreement between Plaintiff and Class Members and Defendant to provide PII, it was the latter's obligation to: (a) use such PHI and PII for business purposes only, (b) take reasonable steps to safeguard that PHI and PII, (c) prevent unauthorized disclosures of the PHI and PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PHI and PII, (e) reasonably safeguard and protect the PHI and PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PHI and PII only under conditions that kept such information secure and confidential.

188. In collecting and maintaining responsibility for the maintenance and protection of the PHI and PII of Plaintiff and the Class and publishing the HIPAA Rights Notice, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiffs and the Class.

189. Plaintiff and the Class fully performed their obligations under the implied contract by providing their PHI and PII to Defendant.

190. Defendant breached the contracts made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class.

191. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity

theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

192. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are at an increased risk of identity theft or fraud.

193. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT VI

Violation of the California Confidentiality of Medical Information Act

(Cal. Civ. Code § 56, *et seq*.)

(On behalf of Representative Plaintiff Kramer and the California Class)

194. Plaintiff, on behalf of himself and the California Class, re-alleges and incorporates the above allegations by reference.

195. Under the California Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.* (hereinafter referred to as the "CMIA"), "medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05.

196. Additionally, Cal. Civ. Code § 56.05 defines "individually identifiable" as meaning that "the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05.

197. Under Cal. Civ. Code § 56.101(a) of the CMIA:

> (a) Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the

> confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.

198. At all relevant times, Defendant was a health care contractor within the meaning of Civil Code § 56.05(d) because it is a "medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care."

199. Plaintiff Kramer and the California Class Members are Defendant's patients, as defined in Civil Code § 56.05(l).

200. Plaintiff Kramer and the California Class Members provided their PII and PHI to Defendant. At all relevant times, Defendant created, maintained, preserved, and stored said PII and PHI information in the ordinary course business.

201. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiff Kramer's and the California Class Members' Private Information without their written authorization violated California Civil Code § 56, *et seq*., and its legal duty to protect the confidentiality of such information.

202. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

203. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff Kramer's and the California Class Members' Private Information was viewed by, released to, and disclosed to third parties without the written authorization of Plaintiff Kramer or the members of the California Class.

204. As a direct and proximate result of Defendant's above-described wrongful actions,

inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff Kramer and the California Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

COUNT VII
Violation of California Consumer Records Act
(Cal. Civ. Code § 1798.82, *et seq.*)
(On behalf of Representative Plaintiff Kramer and the California Class)

205. Plaintiff, on behalf of himself and the California Class, re-alleges and incorporates the above allegations by reference.

206. Section 1798.82 of the California Civil Code, the Consumer Records Act ("CCRA") requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under Cal. Civ. Code § 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

207. Section 1798.82(b) of the California Civil Code provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

208. Cal. Civ. Code § 1798.82(c) required Defendant to issue a security breach notification that complied with the following guidelines:

> (1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2)

> under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
>
> (A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
>
> (B) The title and headings in the notice shall be clearly and conspicuously displayed.
>
> (C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.
>
> (D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

209. The Data Breach described herein constituted a ''breach of the security system" of Defendant, under Cal. Civ. Code §§ 1798.82(a), (b).

210. Upon notification of the breach of security by an unauthorized third party, Defendant knew or had a reasonable belief that the PHI and PII of Plaintiff and Class Members was acquired by an unauthorized person.

211. Despite its knowledge or reasonable belief that Plaintiff's and Class Member's PHI and PII had been acquired by an authorized party when it was informed of the Data Breach, Defendant unreasonably delayed informing Plaintiff Kramer and the California Class about the Data Breach until more than two years after it learned of the Data Breach, in violation of Cal. Civ. Code §§ 1798.82(a), (b).

212. This more than two-year delay after learning of the breach of security was not "the most expedient" time in which Defendant could have disclosed the Data Breach to Plaintiff Kramer and the California Class. *See* Cal. Civ. Code § 1798.82(a),

213. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

214. Upon information and belief, no 1aw enforcement agency instructed Defendant that timely notification to Plaintiff Kramer and the California Class would impede its investigation.

215. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff Kramer and the California Class were deprived of prompt notice of the Data Breach and were thus prevented from taking protective measures, such as monitoring their accounts for signs of fraud, securing identity theft protection, or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff Kramer and the California Class because their stolen information would have had less value to identity thieves.

216. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff Kramer and the California Class suffered increased damages separate and distinct from those caused by the Data Breach itself.

217. Plaintiff Kramer and the California Class seek all remedies available under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiff Kramer and the California Class as alleged above and equitable relief.

218. Defendant's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff Kramer and the California Class of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff Kramer and the California Class and despicable conduct that has subjected Plaintiff Kramer and the California Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff Kramer and the California Class are entitled to punitive damages against Defendant under California Civil Code section 3294(a).

COUNT VIII
Violation of California Unfair Competition Law
(Cal. Bus. & Prof. Code, § 17200, *et seq*.)
(On behalf of Representative Plaintiff Kramer and the California Class)

219. Plaintiff, on behalf of himself and the California Class, re-alleges and incorporates the above allegations by reference.

220. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, *et seq.*) by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a) by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure, release, data breach, and theft; representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of Plaintiff Kramer's and the California Class' Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of their privacy and security protections for the Private Information of Plaintiff Kramer and the California Class;

b) by soliciting and collecting the Private Information of Plaintiff Kramer and the California Class with knowledge that the information would not be adequately protected; and by failing to securely store the Private Information of Plaintiff Kramer and the California Class;

c) by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d) by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*;

e) by violating the CMIA, California Civil Code section 56, *et seq.*; and

f) by violating the CCRA, California Civil Code section 1798.82.

221. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Kramer and the California Class. Defendant's practice was also contrary to legislatively declared and public policies that seek to

protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., CMIA, Cal. Civ. Code, § 56, et seq., and the CCRA, Cal. Civ. Code, § 1798.81.5.

222. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff Kramer and the California Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described above.

223. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff Kramer and the California Class and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Kramer and the California Class.

224. The Plaintiff Kramer and the California Class seek relief under the UCL, including restitution of money or property that Defendant acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DATED: June 20, 2023

Respectfully submitted,

/s/ *Lynn A. Toops*

Lynn A. Toops (No. 26386-49)
Mary Kate Dugan (No. 37623-49)
Natalie A. Lyons (No. 36583-63)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com
nlyons@cohenandmalad.com

Stephen R. Basser*
Samuel M. Ward*
BARRACK, RODOS & BACINE
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659

Counsel for Plaintiff

**Pro Hac Vice* application to be filed